# Listas de control de acceso y fragmentos IP

## Contenido



## Introducción

Este Informe oficial explica los distintos tipos de entradas de Lista de control de acceso (ACL) y lo que sucede cuando distintas clases de paquetes se enfrentan con diferentes entradas. Las ACL se utilizan para bloquear los paquetes IP reenviados por un router.

El RFC 1858 cubre las observaciones de seguridad para el fragmento IP que filtra y resalta dos ataques en los host que implican los fragmentos IP de los paquetes TCP, del ataque del fragmento minúsculo y del ataque del fragmento que solapa. El bloqueo de estos ataques es deseable porque pueden comprometer un host, o inmoviliza a todos sus recursos internos.

El RFC 1858 también describe dos métodos de defensa contra estos ataques, el directo y el indirecto. En el método directo, los fragmentos iniciales que son más pequeños que una longitud mínima se desechan. El método indirecto implica descartar el segundo fragmento de un conjunto de fragmentos, si comienza 8 bytes dentro del datagrama de IP original. Vea por favor el RFC 1858 para más detalles.

Tradicionalmente, los filtros de paquete como los ACL se aplican a los no fragmentos y al fragmento inicial de un paquete del IP porque contienen la capa 3 y la información 4 que los ACL pueden hacer juego contra para una decisión del permit or deny. Los fragmentos no iniciales se permiten tradicionalmente con el ACL porque pueden ser bloqueados sobre la base de la información de la capa 3 en los paquetes; sin embargo, porque estos paquetes no contienen la información de la capa 4, no hacen juego la información de la capa 4 en la entrada ACL, si existe. Permitir los fragmentos no iniciales de un IP datagram es a través aceptable porque el host que recibe los fragmentos no puede volver a montar el datagrama IP original sin el fragmento inicial.

Los Firewall se pueden también utilizar a los bloqueares paquete manteniendo una tabla de fragmentos de paquete puestos en un índice por el IP Address de origen y de destino, el protocolo, y IP ID. El Cisco PIX Firewall y el Firewall del ® del Cisco IOS pueden filtrar todos los fragmentos de un flujo determinado manteniendo esta tabla de información, pero es demasiado

costoso hacer esto en una funcionalidad de ACL del router para básica. El trabajo principal de un Firewall está a los bloqueares paquete, y su rol secundario está a los paquetes de Routes; La tarea principal de un router es rutear paquetes, y su función secundaria es bloquearlos.

Las versiones del IOS de Cisco 12.1(2) y 12.0(11) introdujeron dos cambios a fin de abordar algunos problemas de seguridad en relación con fragmentos TCP. El método indirecto, según lo descrito en el RFC 1858 , fue implementado como parte de la revisión de estado estándar del paquete de entrada TCP/IP. Los cambios también fueron realizados a la funcionalidad de ACL en cuanto a los fragmentos no iniciales.

## Tipos de entradas ACL

Existen seis tipos diferentes de líneas de ACL y cada uno tiene una consecuencia si un paquete coincide o no. En la lista siguiente, el FO = 0 indica un no fragmento o un fragmento inicial en un flujo TCP, el FO > 0 indica que el paquete es un fragmento no inicial, L3 significa la capa 3, y el L4 significa la capa 4.

**Nota:** Cuando hay información de Capa 3 y de Capa 4 en la línea ACL y la palabra clave fragments está presente, la acción de la ACL es conservadora tanto para acciones de admisión como de rechazo. Las acciones son conservadoras por que no deseará negar accidentalmente una porción fragmentada de un flujo porque los fragmentos no contienen la información necesaria para coincidir con todos los atributos del filtro. En el caso de la negación, en vez de negar un fragmento no inicial, se procesa la entrada ACL siguiente. En el caso del permiso, se asume que la información de la capa 4 en el paquete, si está disponible, hace juego la información de la capa 4 en la línea ACL.

### Autorizar la línea ACL sólo con información de L3.

1. Si la información L3 de un paquete hace juego la información L3 en la línea ACL, se permite.
2. Si la información de L3 de un paquete no concuerda con la información de L3 en la línea ACL, se procesa la siguiente entrada ACL.

### Rechazar la línea ACL sólo con información L3.

1. Si la información de un paquete L3 coincide con la información L3 en la línea ACL, se la deniega.
2. Si la información de L3 de un paquete no concuerda con la información de L3 en la línea ACL, se procesa la siguiente entrada ACL.

### Permita la línea ACL con la información L3 solamente, y la palabra clave de los fragmentos está presente

Si la información L3 de un paquete hace juego la información L3 en la línea ACL, se marca el desplazamiento del fragmento del paquete.

1. Si un paquete es FO > 0, el paquete está permitido.
2. Si el FO de un paquete = 0, se procesa la siguiente entrada de ACL.

### Niegue la línea ACL con la información L3 solamente, y la palabra clave de los fragmentos está

presente

Si la información L3 de un paquete hace juego la información L3 en la línea ACL, se marca el desplazamiento del fragmento del paquete.

1. Si el FO de un paquete es > 0, el paquete está denegado.
2. Si el FO de un paquete es igual a 0, se procesa la siguiente línea ACL.

### Permitir la línea ACL con información de las capas 3 y 4

1. Si de un paquete la información el L3 y el L4 hace juego la línea ACL y el FO = 0, se permite el paquete.
2. Si la información de L3 de un paquete coincide con la línea de la ACL y FO > 0, el paquete está permitido.

### Deniegue la línea ACL con información de las capas 3 y 4

1. Si de un paquete la información el L3 y el L4 hace juego la entrada ACL y el FO = 0, se niega el paquete.
2. Si la información L3 de un paquete hace juego la línea ACL y el FO > 0, se procesa la entrada ACL siguiente.

## Diagrama de flujo de las reglas ACL

El siguiente organigrama ilustra las normas sobre ACL que se utilizan al comparar no fragmentos, fragmentos iniciales y fragmentos no iniciales con la ACL.

**Nota:** Los fragmentos no iniciales contienen sólo información de la Capa 3, nunca de la Capa 4, aunque ACL puede contener información de ambas capas 3 y 4.

## Cómo los paquetes pueden coincidir con una ACL

### Ejemplo 1

Los cinco escenarios posibles siguientes implican diversos tipos de paquetes que encuentran el ACL 100. Refiera por favor a la tabla y al organigrama como usted sigue qué sucede en cada situación. La dirección IP del servidor Web es 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

#### El paquete es un fragmento inicial o un no fragmento destinado al servidor en el puerto 80:

La primera línea del ACL contiene el información de las capas 3 y 4, que hace juego el información de las capas 3 y 4 en el paquete, así que se permite el paquete.

#### El paquete es un fragmento inicial o sin fragmento destinado para el servidor en el puerto 21.

1. La primera línea del ACL contiene el información de las capas 3 y 4, pero la información de la capa 4 en el ACL no hace juego el paquete, así que se procesa la línea ACL siguiente.
2. La segunda línea de la ACL deniega a todos los paquetes, de modo que el paquete es denegado.

### El paquete es un fragmento no inicial en el servidor en el flujo de un puerto 80:

La primera línea de la ACL contiene información de capa 3 y capa 4, la información de capa 3 en la ACL coincide con el paquete, la acción de la ACL es permitir, de manera que el paquete sea permitido.

### El paquete es un fragmento no inicial al servidor en un flujo de puerto 21:

La primera línea de la ACL contiene información de la capa 3 y la capa 4. La información de la capa 3 en el ACL coincide con el paquete, no existe información de la capa 4 en el paquete y la acción del ACL es permitir y, por lo tanto, el paquete es permitido.

### El paquete es un fragmento inicial, no es un fragmento o no es un fragmento inicial de otro host en la subred del servidor:

1. La primera línea de la ACL incluye la información de la Capa 3 que no coincide con la información de la Capa 3 en el paquete (la dirección de destino), por esta razón, se procesa la próxima línea de la ACL.
2. La segunda línea de la ACL deniega a todos los paquetes, de modo que el paquete es denegado.

## 'Ejemplo 2'

Los siguientes los mismos cinco escenarios posibles implican diversos tipos de paquetes que encuentran el ACL 101. Refiera una vez más por favor a la tabla y al organigrama como usted sigue qué sucede en cada situación. La dirección IP del servidor Web es 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host
171.16.23.1 eq 80 access-list 101 deny ip any any
```

### El paquete es un fragmento inicial o un destinado no fragmento para el servidor en el puerto 80:

1. La primera línea de ACL contiene información de Capa 3 que coincide con la información de Capa 3 del paquete. La acción ACL es negar, pero porque la palabra clave de los **fragmentos** está presente, se procesa la entrada ACL siguiente.
2. La segunda línea de la ACL contiene información de la Capa 3 y de la Capa 4 la cual coincide con el paquete, por lo tanto el paquete es permitido.

### El paquete es un fragmento inicial o un destinado no fragmento para el servidor en el puerto 21:

1. La primera línea del ACL contiene la información de la capa 3, que hace juego el paquete, pero la entrada ACL también tiene la palabra clave de los **fragmentos**, que no hace juego el paquete porque FO = 0, así que se procesa la entrada ACL siguiente.

2. La segunda línea de la ACL contiene información de la capa 3 y la capa 4. En este caso, la información de la capa 4 no hace juego, así que se procesa la entrada ACL siguiente.
3. La tercera línea del ACL deniega todos los paquetes; por lo tanto, el paquete es denegado

### El paquete es un fragmento no inicial en el servidor en el flujo de un puerto 80:

La primera línea de ACL contiene información de Capa 3 que coincide con la información de Capa 3 del paquete. Recuerde que aunque esto es parte del flujo de un puerto 80, no existe información de Capa 4 en el fragmento no inicial. Se niega el paquete porque la capa 3 coincidencias de la información.

### El paquete es un fragmento no inicial al servidor en un flujo de puerto 21:

La primera línea de la ACL sólo contiene información de la Capa 3 y coincide con el paquete, por lo tanto el paquete es denegado.

### El paquete es un fragmento inicial, no es un fragmento o no es un fragmento inicial de otro host en la subred del servidor:

1. La primera línea de la ACL contiene sólo información de capa 3, y no coincide con el paquete, de manera que se procesa la línea siguiente de la ACL.
2. La segunda línea de la ACL contiene información de la capa 3 y la capa 4. La información de la capa 4 y de la capa 3 en el paquete no hace juego el del ACL, así que se procesa la línea ACL siguiente.
3. La tercera línea del ACL niega este paquete

## Situaciones de ejemplo de palabras clave de fragmentos

### Escenario 1

El router B conecta con un servidor Web, y el administrador de la red no quiere permitir que ninguna fragmentos alcancen el servidor. Este escenario muestra qué sucede si el administrador de la red implementa el ACL 100 contra el ACL 101. El ACL es entrante aplicado en la interfaz del serial0 del Routers (s0) y debe permitir que solamente los paquetes NON-hechos fragmentos alcancen al servidor Web. Consulte el diagrama de flujo de reglas de ACL y las secciones Cómo los paquetes pueden coincidir con una ACL mientras sigue la situación.

### Consecuencias de la utilización de la palabra clave fragmentos

La siguiente es la ACL 100:

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

La primera línea de la ACL 100 permite únicamente el HTTP al servidor, pero también admite los fragmentos no iniciales a cualquier puerto del TCP en el servidor. Permite estos paquetes porque los fragmentos no iniciales no contienen la información de la capa 4, y la lógica ACL asume que si las coincidencias de la información de la capa 3, después la información de la capa 4 también haría juego, si estaba disponible. La segunda línea es implícita y niega todo el otro tráfico.

Es importante observar que, a partir de los Cisco IOS Software Releases 12.1(2) y 12.0(11), el nuevo código ACL cae los fragmentos que no hacen juego ninguna otra línea en el ACL. Las versiones anteriores permiten los fragmentos no iniciales a través si no hacen juego ninguna otra línea del ACL.

El siguiente es ACL 101:

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host 171.16.23.1 eq 80 access-list 101 deny ip any any
```

El ACL 101 no permite los fragmentos no iniciales a través al servidor debido a la primera línea. Un fragmento no inicial al servidor se niega cuando encuentra la primera línea ACL porque la información de la capa 3 en el paquete hace juego la información de la capa 3 en la línea ACL.

La inicial o los no fragmentos al puerto 80 en el servidor también hace juego la primera línea del ACL para la información de la capa 3, pero porque la palabra clave de los fragmentos está presente, se procesa la entrada ACL siguiente (la segunda línea). La segunda línea de la ACL permite los fragmentos iniciales o no iniciales porque concuerdan con la línea ACL para la información de las Capas 3 y 4.

Los fragmentos no iniciales destinados a los puertos TCP de otros host en la red de 171.16.23.0 son bloqueados por este ACL. La información de la Capa 3 en estos paquetes no coincide con la información de la Capa 3 en la primera línea ACL, entonces se procesa la siguiente línea ACL. La información de Capa 3 en estos paquetes tampoco coincide con la información de Capa 3 en la segunda línea ACL, por lo tanto se procesa la tercera línea ACL. La tercera línea está implícita y niega todo el tráfico.

El administrador de la red en este escenario decide implementar ACL 101 porque permite que sólo los flujos HTTP no fragmentados ingresen en el servidor.

## Escenario 2

Un cliente tiene conectividad a Internet en dos diversos sitios, y hay también una conexión backdoor (Puerta de servicio) entre los dos sitios. La directiva del administrador de la red es permitir que el grupo A en el sitio 1 acceda al servidor HTTP en el sitio 2. El Routers en ambos sitios está utilizando las direcciones privadas (RFC 1918 ) y el Network Address Translation (NAT) para traducir los paquetes que se rutean a través de Internet.

El administrador de la red en el sitio 1 es Policy Routing las direcciones privadas asignadas para agrupar A, de modo que él utilice la entrada posterior con el serial0 del router a (s0) al acceder al servidor HTTP en el sitio 2. El router en el sitio 2 tiene una Static ruta a 172.16.10.0, para rutear el tráfico de retorno para agrupar A también con la entrada posterior. El resto del tráfico es procesado por el NAT y ruteado a través de Internet. En este escenario, el administrador de red debe decidir qué aplicación o qué flujo funcionará si se fragmentan los paquetes. No es posible hacer el HTTP y el trabajo de los flujos del File Transfer Protocol (FTP) al mismo tiempo porque uno o el otro se rompe.

Consulte el diagrama de flujo de reglas de ACL y las secciones Cómo los paquetes pueden coincidir con una ACL mientras sigue la situación.

### Explicación de las opciones del administrador de la red

En el siguiente ejemplo, el Route Map llamado FOO en el router A envía los paquetes que hacen juego el ACL 100 a través al router B con el s0. Todos los paquetes que no hacen juego son procesados por el NAT y tomar la ruta predeterminado a través de Internet.

Nota: Si un paquete se cae de la parte inferior del ACL, o es negado por él, después directiva-no se rutea.

Lo que sigue es una configuración parcial del router A, mostrando que un route-map de la directiva llamado FOO está aplicado para interconectar el e0, donde el tráfico del grupo A ingresa al router:

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq
80 access-list 100 deny ip any any
```

El ACL 100 no prohibe a Policy Routing en ambos la inicial, los no fragmentos y los fragmentos no iniciales del HTTP fluyen al servidor. La inicial y los no fragmentos de los flujos HTTP al servidor son permitidos por el ACL y la directiva ruteados porque hacen juego el información de las capas 3 y 4 en la primera línea ACL. Los fragmentos no iniciales son permitidos por el ACL y la directiva ruteados porque la información de la capa 3 en el paquete también hace juego la primera línea ACL; la lógica ACL asume que la información de la capa 4 en el paquete también haría juego si estaba disponible.

Nota: El ACL 100 rompe otros tipos de flujos hechos fragmentos TCP entre el grupo A y el servidor porque la inicial y los fragmentos no iniciales consiguen al servidor a través de diversas trayectorias; los fragmentos iniciales son procesados por el NAT y ruteados a través de Internet, pero los fragmentos no iniciales del mismo flujo son directiva ruteada.

Las ayudas hechas fragmentos de un flujo FTP ilustran el problema en este escenario. Los fragmentos iniciales de un flujo FTP coinciden con la información de la Capa 3 pero no con la información de la Capa 4 de la primera línea ACL y posteriormente son denegados por la segunda línea. Estos paquetes son procesados por NAT y enrutados a través de Internet.

Los fragmentos no iniciales de una coincidencia del flujo FTP la información de la capa 3 en la primera línea ACL, y la lógica ACL asume una coincidencia positiva en la información de la capa 4. Estos paquetes están enrutados por política, y el host que reensambla estos paquetes no reconoce los fragmentos iniciales como parte del mismo flujo que los fragmentos no iniciales enrutados por política porque NAT ha cambiado la dirección de origen de los fragmentos iniciales.

El ACL 100 en la configuración abajo repara el problema de FTP. La primera línea de ACL 100 niega los fragmentos iniciales y NON-iniciales FTP del grupo A al servidor.

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1
fragments access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80 access-list
100 deny ip any any
```

Los fragmentos iniciales hacen juego en la información de la capa 3 en la primera línea ACL, pero la presencia de la palabra clave de los fragmentos hace la línea ACL siguiente ser procesada. El fragmento inicial no hace juego la segunda línea ACL para la información de la capa 4, y así que la línea implícita siguiente del ACL se procesa, que niega el paquete. Los fragmentos no iniciales hacen juego la información de la capa 3 en la primera línea del ACL, así que se niegan. Rubrique y los fragmentos no iniciales son procesados por el NAT y ruteados a través de Internet, así que el servidor no tiene ningún problema con el nuevo ensamble.

Reparar los flujos FTP HTTP hecho fragmentos las roturas fluye porque los fragmentos HTTP iniciales ahora son directiva ruteada, pero los fragmentos no iniciales son procesados por el NAT y ruteados a través de Internet.

Cuando un fragmento inicial de un flujo HTTP del Grupo A al servidor se enfrenta con la primera línea del ACL, coincide con la información de Capa 3 en el ACL, pero debido a la palabra clave fragments, se procesa la siguiente línea del ACL. La segunda línea de la ACL permite y la política enruta el paquete al servidor.

Cuando los fragmentos HTTP no iniciales destinados desde el Grupo A al servidor se enfrentan con la primera línea del ACL, la información de Capa 3 en el paquete coincide con la línea ACL y se rechaza el paquete. NAT procesa estos paquetes que atraviesan Internet para llegar al servidor.

El primer ACL en este escenario permite los flujos hechos fragmentos HTTP y rompe los flujos FTP hechos fragmentos. La segunda ACL permite los flujos fragmentados de FRP e interrumpe los flujos fragmentados de HTTP. Los flujos de TCP se interrumpen en cada caso porque los fragmentos iniciales y no iniciales toman diferentes trayectos hacia el servidor. El reensamblado no es posible porque NAT cambió la dirección de origen de los fragmentos no iniciales.

No es posible construir una ACL que permita ambos tipos de flujos fragmentados hacia el servidor, entonces el administrador de red debe elegir con qué flujo quiere trabajar.

## Información Relacionada

- Página de Soporte de IP Routing
- Soporte Técnico y Documentación - Cisco Systems